IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 11-272
	)	
RICHARD STANLEY	)	

UNITED STATES PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING THE DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The defendant, Richard Stanley, has been indicted for possessing visual depictions of minors engaged in sexually explicit conduct. On April 13, 2012, Mr. Stanley filed a "Motion to Suppress Evidence" (Document 24). On May 24, 2012, this Court conducted a hearing on Mr. Stanley's motion. The United States submits these proposed findings of fact and conclusions of law to assist the Court in resolving the motion.

I. FINDINGS OF FACT – INTERNET CONNECTION

1. On November 11, 2010, Cpl. Robert Erdely of the Pennsylvania State Police Computer Crime Unit was investigating the use of internet file-sharing software, such as Limewire, to distribute child pornography files over peer-to-peer file-sharing networks, such as Gnutella.(6-7)[1]

2. Cpl. Erdely is a certified computer forensic examiner who has testified as an expert in online investigations in federal and

[1] Parenthetical numerical references herein refer to the applicable pages of the transcript of the suppression hearing that occurred on May 24, 2012. References to exhibit numbers refer to the exhibits presented during the suppression hearing.

state courts. (5-6, Ex. 8)

3. Peer-to-peer file-sharing has become a common means by which child pornography files are downloaded from the internet and thereafter shared with others over the internet. (Ex. 8)

4. As Cpl. Erdely was conducting his investigation on November 11, 2010, he identified a computer connected to the internet and the Gnutella file-sharing network sharing 77 files ("the Subject Computer"). (6)

5. One of the files was titled "9yo Jenny nude with legs spread wide apart showing pussy – underage lolita R@ygold pthc ptsc ddogprn pedo young child sex preteen hussyfan kiddie kiddy porn.jpg." (10-11, Ex. 8)

6. The file depicts a nine-year-old pre-pubescent female child on a bed with her genitals exposed, with her hands tied above her head, and with her legs tied and spread apart. (11, Ex. 8)

7. Computers operating file-sharing software for the Gnutella file-sharing network are assigned a globally unique ID ("GUID"). (9)

8. The GUID identifies a particular computer on the file-sharing network and stays with the computer even after a particular file-sharing session is completed. (9, 19-20)

9. Cpl. Erdely identified the GUID for the computer sharing the child pornography file referenced above as 8754E6525772BA0134C4C6CACF12E300 ("the Subject GUID"). (Ex. 8)

10. A computer connected to the internet is assigned an internet protocol address ("IP address") so that internet data can be accurately sent to and from a particular computer or network. (8-10)

11. Cpl. Erdely identified the IP address assigned to the computer on November 11, 2010, as 98.236.6.174 ("the November 11 IP address"). (11-12, Ex. 8).

12. Cpl. Erdely then researched the November 11 IP address via public business records and determined that it was an address that Comcast assigns to its customers. (11-12, Ex. 8)

13. Cpl. Erdely thereafter obtained a court order directing Comcast to disclose which customer the November 11 IP address was assigned to on November 11, 2010. (6)

14. Comcast responded to the court order by identifying the customer as William Kozikowski of XXXX (redacted) Dormont Avenue, Pittsburgh, PA ("the Kozikowski residence"). (12)

15. Cpl. Erdely then obtained a state search warrant for the Kozikowski residence. (12)

16. On November 18, 2010, Cpl. Erdely served the search warrant at the Kozikowski residence. (12)

17. Two computers were inside the residence. (12)

18. Cpl. Erdely concluded that neither computer was the Subject Computer because neither of them contained internet file-sharing software with the Subject GUID. (12-13, 21)

19. Cpl. Erdely then reviewed the internet router at the Kozikowski residence and observed that it set up a wireless network at the residence that was not encrypted or password-protected. (13)

20. Similar to an unlocked exterior door, someone could unlawfully trespass into the Kozikowski home network without having to force entry. (13, 17)

21. William Kozikowski agreed to allow Cpl. Erdely access to the router at the Kozikowski residence in the future to determine who had trespassed on the Kozikowski home network and thereby shared child pornography over the internet. (14)

22. On January 19, 2011, two additional computer crime investigators identified the Subject Computer sharing child pornography files over the internet via the Gnutella network. (18, 21)

23. Paula Hoffa, an investigator in Wisconsin, observed a computer with the Subject GUID that was connected to the internet via the IP address 98.239.133.215 ("the January 19 IP address"). (18)

24. The Subject Computer was sharing a file named "pictures from ranchi torpedo dloaded in 2009- pedo kdv kidzilla pthc toddlers 0yo 1yo 2yo 3yo 4yo 5yo 6yo 9yo tara babyj (220).jpg". (25, Ex. 8)

25. The file depicts an approximately 3 to 4 year old naked female

child with her genitals exposed and an adult hand. (Ex. 8)

26. Also on January 19, 2011, Jessica Eger, an investigator with the Pennsylvania Attorney General's Office, located a computer with the Subject GUID sharing a file over the internet titled "pthc Pedoland Frifam 5yo MG (CP high qual, HC-suck) -tc.mpg". (18, 25, Ex. 8)

27. The file contains a video of an approximately 9-year-old nude prepubescent female child bent over with her pubic area exposed and with another person touching the child's vagina, and the child is then shown kissing a penis and putting it in her mouth with her hand. (Ex. 8)

28. Cpl. Erdely responded to these developments by traveling back to the Kozikowski residence during the evening of January 19, 2011. (22)

29. Cpl. Erdely reviewed the Kozikowski router data and confirmed that the January 19 IP address through which the investigators had identified the Subject Computer sharing the child pornography files that day was assigned to the Kozikowski home network. (22-24)

30. Cpl. Erdely further confirmed from the Kozikowski router data that there was an unauthorized wireless device connected to the internet through the Kozikowski router and the Kozikowski IP address. (22-24)

31. The router data revealed the serial number of the wireless

card, also known as the MAC address, for the device that was trespassing on the Kozikowski home network. (22-24)

32. The router data also revealed that that wireless device was receiving internet data through a port on the device that is commonly used to download files over the Gnutella file-sharing network. (24, Ex 8)

33. If an IP address is to a computer connected to the internet as a mailing address is to a residence, then a port is to a computer connected to the internet as an external door is to a residence – except that the residence would have to have over 65,000 external doors because there are over 65,000 ports through which internet data can be transmitted to a computer connected to the internet. (10)

34. In light of the particular Gnutella port being utilized by the wireless device that was trespassing on the Kozikowski home network as well as all of the other information generated during the investigation, Cpl. Erdely concluded that the wireless device was the Subject Computer. (26, Ex. 8)

35. In addition, the wireless device was trespassing on the Kozikowski home network and stealing an internet connection from Comcast and Mr. Kozikowski. (26)

36. At that time (i.e., during the evening of January 19, 2011), Cpl. Erdely used Moocherhunter – a freely available internet application that locates wireless signals similar to many

other commonly and widely used applications – and a common antenna to follow the stolen internet connection across the street from the Kozikowski residence to the front door of Mr. Stanley's residence ("the Stanley residence"). (26-30)

37. Cpl. Erdely had Moocherhunter downloaded on his computer and, as noted above, had identified the MAC address of the wireless device from data on the Kozikowski router. (26-30)

38. Cpl. Erdely entered the MAC address into Moocherhunter, held his computer and the antenna in his hands, pointed the antenna at the Kozikowski residence, and observed the Moocherhunter power meter relative to the stolen internet connection. (26-30)

39. Cpl. Erdely then pointed the antenna away from the Kozikowski residence and the power meter rose to the level 67. (26-30, 55-57, Exs. 5-7)

40. As Cpl. Erdely thereafter walked toward the apartment building across the street containing the Stanley residence, the power meter began to rise. (26-30, 55-57, Exs. 5-7)

41. When Cpl. Erdely stood on the public sidewalk directly in front of the Stanley residence about 15 feet from the front door and pointed the antenna at the residence, the power meter rose to level 100 which is the highest possible reading. (26-30, 55-57, Exs. 5-7)

42. There was no other apartment in the vicinity of where Cpl.

Erdely pointed the antenna at that time. (26-30, 55-57, Exs. 5-7)

43. Based upon his training and experience, Cpl. Erdely reached the conclusion that he had successfully followed the stolen internet connection from the Kozikowski home network to the front door of the Stanley residence.(26-30)

44. Technology that allows for the detection and location of wireless signals is freely available and commonly used by people in everyday life. (32-53)

45. For example, there are free applications for smart phones that allow people to identify who is "mooching" off their network or to identify available wireless signals. (32-53)

46. In addition, unless a user of a laptop computer with wireless internet connectivity turns off the function, a pop-up message will commonly appear on the screen identifying nearby wireless signals and the respective signal strengths – if a user chooses to move to a nearby location, the wireless signal strength indicators will adjust depending upon whether the user walked closer to or farther away from a particular signal. (32-53)

47. Moocherhunter is a particular application of this technology. (32-53)

48. Moocherhunter, itself, may not be generally used by the public to detect and locate wireless signals, but the technology that

supports Moocherhunter and the other applications referenced above is now generally used by the public, as well as by telephone, internet, and television service providers, to detect and locate wireless signals. (32-53)

49. As a result of this general public use, most people understand that the wireless signals they deliberately transmit using their computers, cell phones, and televisions, can be, and often are, detected and located.

50. In fact, most people understand that their wireless signals have to be detected and located for their wireless devices to operate properly.

51. Therefore, as a factual matter, an expectation that a wireless internet signal that is deliberately transmitted beyond one's residence will remain undetected or its location undetermined, even if subjectively held, is not objectively reasonable.

52. Such an expectation becomes even less reasonable if the wireless internet signal was not only transmitted beyond one's residence but was also connected to someone else's wireless network without authorization.

II. CONCLUSIONS OF LAW – INTERNET CONNECTION

A. No Fourth Amendment "Search"

1. It is Mr. Stanley's burden to establish that a Fourth Amendment search occurred prior to requiring the prosecution to demonstrate that a search was reasonable. *See Rawlings v.*

Kentucky, 448 U.S. 98, 104 (1980); *United States v. Salvucci*, 448 U.S. 83, 85 (1980); and *Rakas v. Illinois*, 439 U.S. 128, 131 n.1 (1978).

2. A Fourth Amendment search can occur in two ways. *Free Speech Coalition v. Attorney General*,677 F.3d 519, 543 (3d Cir. 2012).

3. First, when the particular defendant can establish that his reasonable expectation of privacy was invaded by government action. *Id*.

4. A reasonable expectation of privacy requires both an actual subjective expectation and an expectation that is objectively justifiable under the circumstances. *Id*.

5. The second way in which a Fourth Amendment search can occur is when a governmental actor "unlawfully, physically occupies private property for the purpose of obtaining information". *Id*.

6. Common-law trespass to obtain information is required. *Id*.

7. The use of Moocherhunter did not result in an unlawful physical occupation of private property or any common-law trespass.

8. Therefore, the particular use of Moocherhunter in this case can only be a search if it intruded upon a reasonable expectation of privacy.

9. Such an intrusion cannot be shown based upon speculation about

how Moocherhunter could potentially have been used.

10. The only relevant consideration is what information was obtained in this case (i.e., the direction of a stolen internet connection – its existence was identified from the data on the Kozikowski router). (27-30)

11. As the Supreme Court has explained, "we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment." *United States v. Karo*, 468 U.S. 705, 712 (1984); *see also United States v. Diaz-Castaneda*, 494 F.3d 1146, 1152 (9th Cir. 2007) ("[T]he possibilities of database error and police officer abuse, while real, do not create a legitimate expectation of privacy where none existed before. Government actions do not become Fourth Amendment searches simply because they might be carried out improperly.").

12. Mr. Stanley rests his motion largely upon the Supreme Court's opinion in *Kyllo v. United States*, 533 U.S. 27 (2001).

13. *Kyllo* involved the use of a thermal-imaging device initially and deliberately aimed at a residence to detect the heat inside the residence. *Id.* at 29-31.

14. There is a surface-level similarity between *Kyllo* and this case.

15. Upon close examination, however, the investigative steps taken in *Kyllo* are revealed as fundamentally the opposite of the

investigative steps taken in this case.

16. That is, the agents in *Kyllo* began by focusing upon a particular residence and then used a device to explore the details of what was occurring inside. *Id.* at 29-30.

17. In this case, Cpl. Erdely began by focusing on a stolen internet connection in a public space and then used a device to determine its direction. (26-30)

18. As soon as the direction of the connection led Cpl. Erdely to the exterior of Mr. Stanley's residence, Cpl. Erdely stopped using the device and applied for a search warrant. (29)

19. Significantly, the Supreme Court in *Kyllo* held that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id*. at 40 (emphasis added).

20. Cpl. Erdely did not use Moocherhunter to "explore details" of Mr. Stanley's residence.

21. To the contrary, Cpl. Erdely used Moocherhunter to explore details of the internet connection in public space and stopped as soon as the connection led to Mr. Stanley's residence.

22. The fact that Cpl. Erdely was able to connect the internet connection to Mr. Stanley's residence does not mean that he explored the details of the residence.

23. Moreover, as indicated by the importance the Supreme Court in *Kyllo* placed upon general public usage and its reference to *California v. Ciraolo*, 476 U.S. 207 (1986), *Kyllo* is a case that is merely a particular application of the reasonable expectation of privacy test stated above. *See Kyllo*, 533 U.S. at 39-40 & n.6.

24. The Court in *Kyllo* did not create a new Fourth Amendment search test, but, instead, applied the existing reasonable expectation of privacy test to conclude that a resident has a reasonable expectation of privacy in the amount of heat inside a residence and not being deliberately blown into, or stolen from, the neighbor's house next door.

25. There is good reason to conclude that if *Kyllo* involved the use of a thermal imaging device to follow the heat that a person was deliberately stealing from, or blowing into, a neighbor's house, the result would have been different.

26. Under those circumstances, the use of the thermal imaging device to follow the heat to the residence would not be an exploration of the details of the residence and the person would not have a reasonable expectation of privacy in the direction of the stolen or trespassing heat.

27. Many cases since *Kyllo* support these conclusions.

28. For example, in *Illinois v. Caballes*, 543 U.S. 405, 408-10 (2005), the Supreme Court upheld the warrantless dog sniff of

a vehicle during a traffic stop despite a *Kyllo*-based challenge.

29. The Court distinguished *Kyllo* by noting that the thermal imaging device used in *Kyllo* detected heat levels, not necessarily illegal activity; whereas the dog sniff was limited to detecting illegal activity (i.e., drug possession). *Id*. 409-10.

30. The Court in *Caballes* explained "any interest in possessing contraband cannot be deemed legitimate, and thus, governmental conduct that only reveals the possession of contraband compromises no legitimate privacy interest. This is because the expectation that certain facts will not come to the attention of the authorities is not the same as an interest in privacy that society is prepared to consider reasonable." *Id*. at 408-09 (citations and quotations omitted).

31. Subsequent appellate and district court opinions have extended the rationale in *Caballes* from vehicles to residences. *See United States v. Brock*, 417 F.3d 692, 695-96 (7th Cir. 2005) (citing multiple cases and refusing to follow the contrary decision of the Second Circuit in *United States v. Thomas*, 757 F.2d 1359, 1366-67 (2d Cir. 1985)).

32. The United States District Court for the District of New Jersey recently held in *United States v. Anthony*, 2012 WL 959448, *5-7 (D.N.J. March 20, 2012), that a dog sniff at the

door of a private residence was not a search because the only information that was revealed was "information in which no person has a legitimate expectation of privacy".

33. The district court noted that "neither the Supreme Court nor the Third Circuit Court of Appeals has had occasion to apply *Caballes* to a dog sniff at a private residence, but the majority of authorities point to the no expectation of privacy in contraband reasoning from the Supreme Court in holding that dog sniffs are not searches even when the thing being sniffed is the outside of a private residence instead of a car." *Id.* at 5.

34. The district court went on to convincingly reject the contrary conclusions of the Second Circuit in *United States v. Thomas*, 757 F.2d 1359, 1366-67 (2d Cir. 1985), and of the Florida Supreme Court in *Jardines v. State*, 73 So.3d 34 (Fla.2011) (cert. granted in part *Florida v. Jardines*, 132 S.Ct. 995 (2012)).

35. Cpl. Erdely's use of Moocherhunter only revealed information in which no person has a legitimate expectation of privacy.

36. That is, only the direction of the stolen internet connection was obtained through the use of Moocherhunter.

37. Mr. Stanley did not have an expectation of privacy in the contraband internet connection.

38. Therefore, under *Caballes* and the cases applying it, Cpl.

Erdely did not search the Stanley residence when he followed the stolen internet connection to outside the front door.

39. In addition to the *Caballes* line of cases, several other opinions support the conclusion that Mr. Stanley had no reasonable expectation of privacy in the information obtained using Moocherhunter.

40. In *United States v. Caymen*, 404 F.3d 1196, 1200-01 (9th Cir. 2005), the defendant claimed that the laptop he had possessed was unlawfully searched without a valid warrant.

41. The Ninth Circuit rejected the claim and refused to even recognize that a search had occurred because the defendant had obtained possession of the laptop by fraud. *Id*.

42. The court explained, "[t]he Fourth Amendment does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that society is prepared to accept as reasonable. A legitimate expectation of privacy means more than a subjective expectation of not being discovered." *Id*. at 1200 (quotation marks omitted).

43. If the defendant in *Caymen* had no basis to legitimately object to a search of his laptop because of the fraudulent manner in which he acquired it, Mr. Stanley has no basis to legitimately object to Cpl. Erdely following the stolen internet connection

to the outside of the Stanley residence.

44. Mr. Stanley cannot credibly argue that he had a reasonable expectation of privacy in the direction of the stolen internet connection when the very existence of the connection was a product of trespass and theft.

45. As the Seventh Circuit explained in *United States v. Simms*, 626 F.3d 966, 969 (7th Cir. 2010), "[w]e cannot see how an expectation of privacy that can be realized only by breaking the law can be considered reasonable and therefore protected by the Constitution, unless the law in question is invalid."

46. It should be emphasized that not only did Mr. Stanley steal the internet connection, but he trespassed into the Kozikowski home network to do so.

47. The trespass connected Mr. Stanley's computer with the Kozikowski computers via the home network.

48. By doing so, Mr. Stanley made the content of his internet traffic available to the other users of the Kozikowski home network via freely available software. (53-54)

49. As a result, Mr. Stanley not only had no reasonable expectation of privacy in the existence or direction of the stolen internet connection, he had no reasonable expectation of privacy in the content of the internet traffic that was flowing through the trespassed network to his computer via the stolen internet connection.

50. This conclusion is supported by the Eleventh Circuit's opinion in *United States v. King*, 509 F.3d 1338, 1339, 1341-42 (11th Cir. 2007).

51. The defendant in *King* knowingly connected his computer to the network for the military base where he was residing. *Id.* at 1339-40.

52. The defendant understood that his online activities could be monitored but believed that he had configured his computer so that it could not be accessed through the network. *Id.*

53. The computer, however, could be, and was, accessed through the network resulting in the eventual discovery of child pornography evidence. *Id.*

54. The defendant thereafter argued that the warrantless review of the contents of his computer via the network was an unlawful search because he connected his computer to the network with the understanding that his computer could not be accessed. *Id.* at 1341.

55. The Eleventh Circuit recognized that the defendant may have had a subjective expectation of privacy in his networked computer. *Id.* at 1341-42.

56. The court refused, however, to find the expectation objectively reasonable because it was a part of the network to which the defendant knowingly connected even if he did so with the understanding that his computer could not be accessed over

the network. *Id.* at 1342.

57. Like the defendant in *King*, Mr. Stanley knowingly connected his computer to a network the investigation of which led to his front door.

58. Under *King*, he not only had no reasonable expectation of privacy in the existence or direction of the stolen internet connection, he had no reasonable expectation of privacy in the internet traffic through the connection even if he was not aware that his internet traffic was accessible.

B. No Exclusion of Evidence

1. No evidence should be excluded even if Cpl. Erdely's use of Moocherhunter to follow the internet connection was a Fourth Amendment search.

2. The Fourth Amendment requires reasonableness, not necessarily warrants. *Scott v. Harris*, 550 U.S. 372, 383 (2007); *United States v. Sims*, 553 F.3d 580, 582 (7th Cir. 2009).

3. Reasonableness determinations under the Fourth Amendment "nearly always involve examination of the totality of the circumstances, because the Amendment recognizes that no single set of legal rules can capture the ever changing complexity of human life." *United States v. Price*, 558 F.3d 270, 278 n.6 (3d Cir. 2009).

4. Mr. Stanley's argument that a search warrant was required to make Cpl. Erdely's use of Moocherhunter reasonable begs the

question of whether a search warrant could have been obtained.

5. As further discussed below, there was probable cause to support a search warrant application.

6. Under the circumstances that existed at the time, however, a search warrant would have had to have been obtained for every residence within a particular radius of the Kozikowski residence because, until the internet connection was followed to Mr. Stanley's residence, the direction of the connection was not known. (31)

7. It would have been clearly impractical to the point of impossible for Cpl. Erdely to obtain a search warrant for each of the residences within a particular radius of the Kozikowski residence.

8. Such a radius would have easily included 25 or more residences in light of the fact that the Kozikowski residence was surrounded by other residences. (31)

9. The process of identifying and particularly describing the residences would have alone taken days. (31)

10. By that time, the stolen internet connection would likely have evaporated.

11. An argument could perhaps be made that Cpl. Erdely could have obtained one search warrant for the neighborhood.

12. Doing so, however, would not have addressed Mr. Stanley's objection because, according to Mr. Stanley, the use of

Moocherhunter was a search of his residence, not of the neighborhood around his residence.

13. In any event, a neighborhood is a public place and, therefore, no warrant was needed to search it.

14. It was, therefore, reasonable for Cpl. Erdely, in possession of probable cause of the ongoing criminal activity referenced herein, to use Moocherhunter to follow the internet connection in the manner that he did even if doing so was a Fourth Amendment search.

15. Under the circumstances, it would be completely unjustified to impose the severe sanction of exclusion of evidence.

16. The Supreme Court has stated that application of the exclusionary rule to challenged evidence "must be weighed against its substantial social costs." *Herring v. United States*, 129 S.Ct. 695, 700-01 (2009) (quoting *Illinois v. Krull*, 480 U.S. 340, 353-53 (1987)).

17. The balancing that must take place prior to the application of the exclusionary rule should focus upon the degree of deliberateness and culpability of the particular law enforcement conduct and the cost of "letting guilty and possibly dangerous defendants go free – something that offends basic concepts of the criminal justice system." *Herring*, 129 S.Ct. at 700-02.

18. Application of the exclusionary rule should be the "last

resort" and is not an individual right. *Id.* at 700.

19. It should be applied only when its application would result in "appreciable deterrence" and not simply when some level of marginal deterrence could result from its application. *Id.*

20. "[W]hen police mistakes are the result of negligence . . . rather than systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not 'pay its way.'" *Id.* at 704 (citing *United States v. Leon*, 468 U.S. 897, 907-08 (1984)).

21. Assuming *arguendo* that the Fourth Amendment requires a search warrant for the use of Moocherhunter to follow a stolen internet connection, application of the exclusionary rule plainly should not occur in Mr. Stanley's case in light of the Supreme Court's holdings in *Herring v. United States*, 129 S.Ct. 695, 700-01 (2009), and more recently in *Davis v. United States*, 131 S.Ct. 2419 (2011).

22. Under the specific and difficult circumstances, Cpl. Erdely's decision to utilize Moocherhunter, after receiving the advice of the assigned prosecutor, instead of attempting to obtain over 25 search warrants before the stolen internet connection evaporated is not at all the type of conduct that the exclusionary rule was developed to deter. (26, 31)

23. Moreover, Mr. Stanley's argument that Cpl. Erdely should have obtained a tracking device warrant prior to using

Moocherhunter gets no further than the definition of a "tracking device".

24. The applicable definition of "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 Pa.C.S.A. § 3117(b) (emphasis added).

25. Cpl. Erdely's use of Moocherhunter does not fit within any logical construction of this definition.

26. Mr. Stanley has not adequately identified any movement of any person or object that was tracked or that was intended to be tracked.

27. Cpl. Erdely used Moocherhunter to identify the direction of an internet connection in a single public space on a single occasion.

28. The internet connection was not moving, was not a person or an object, and its movement was not tracked.

29. Furthermore, the movement of the Subject Computer was never tracked.

30. The tracking of the movement of an object associated with a person is what potentially triggers a Fourth Amendment event in the tracking device context because such location tracking implicates the person's, as opposed to the object's, privacy interests.

31. The use of a device to reveal the location of a particular

object on a single occasion does not trigger a Fourth Amendment event in the tracking device context because no movement of the object, and hence the person, is tracked.

32. Whether the revelation of the location of the object on a single occasion is otherwise a Fourth Amendment event depends, as explained above, on whether a Fourth Amendment search occurred.

33. The many and varied opinions relied upon by Mr. Stanley that involve location information for electronic devices are inapposite because they involve the acquisition of such information over the course of time that potentially revealed the movement of a particular object, and hence a person, over that course of time.

34. Even the District Court of Arizona's decision in *United States v. Rigmaiden*, 844 F.Supp.2d 982, 987, 995-96 (D.AZ. 2012), is inapposite here because that case involved the use of a cell site simulator on several occasions in several locations to track the movement of a Verizon Wireless aircard in the defendant's computer for the purpose of tracking and eventually arresting the defendant.

35. *Rigmaiden* involved the tracking of movement of an object on several occasions in several locations. *Id.* at 995.

36. It should be noted that the prosecution in *Rigmaiden* asserted a qualified law enforcement privilege to avoid disclosing the

specifications of the cell site simulator and, in conjunction therewith, made a limited concession that the use of the cell site simulator was a Fourth Amendment search in that case to avoid further litigation that could have defeated the privilege. *Id.* at 995-96 & n.6.

37. Moreover, the cell site simulator used in *Rigmaiden* did not identify the direction of a pre-existing signal, but, instead, caused a signal to be transmitted that was then analyzed. *Id.* at 995.

38. In light of the foregoing, the acquisition of a tracking device warrant was not a realistic option for Cpl. Erdely because he had no intention of tracking the movement of any object or person and did not track the movement of any object or person using Moocherhunter.

39. It should be noted that the foundation of Mr. Stanley's tracking device argument is that whenever the use of an electronic or mechanical item results in the location of an object, the item is a tracking device – even if the movement of the object itself was never actually tracked.

40. This argument is a reductio ad absurdum that contradicts the plain meaning of the applicable tracking device definition stated above, would lead to inane conclusions, and must be rejected.

41. According to this argument, the use of a telephone to call a

suspect's home or work telephone number would make the telephone a tracking device if it reveals that the suspect is at home or at work – even the use of a flashlight to illuminate a suspect's footprints leading through the curtilage to the front door of a residence would make the flashlight a tracking device of the suspect.

42. In addition, it should be noted that Mr. Stanley's argument that a tracking device warrant should have been obtained is not consistent with his argument that Cpl. Erdely's use of Moocherhunter was a Fourth Amendment search of his residence under *Kyllo*.

43. If Cpl. Erdely had obtained a tracking device warrant, somehow particularly identifying "the person or property to be tracked", it is quite likely that Mr. Stanley would still argue that a traditional search warrant for his residence, not a tracking device warrant, was necessary. *See* Fed.R.Crim.P. 41.

III. FINDINGS OF FACT – SEARCH WARRANT

1. After Cpl. Erdely followed the internet connection to the exterior of Mr. Stanley's residence, he promptly prepared a state search warrant and supporting affidavit on scene and presented the documents to a Pennsylvania district justice. (29, 58, Ex. 8)

2. After explaining in the supporting affidavit his computer

crime expertise, the significance of internet terms such as IP addresses and GUID's, and how internet file-sharing networks operate, Cpl. Erdely stated what he termed the "Specific Probable Cause" information pertaining to the Stanley residence. (Ex. 8)

3. This information included the details of Cpl. Erdely's online investigation on November 11, 2010, during which he identified the Subject Computer with the Subject GUID sharing child pornography files over a Comcast IP address assigned to the Kozikowski home network. (Ex. 8)

4. Cpl. Erdely also included the details of the subsequent service of the search warrant at the Kozikowski residence during which he was able to determine that none of the Kozikowski computers was the Subject Computer and that the Kozikowski router had set up a wireless home network that was not protected by encryption or a password. (Ex. 8)

5. Cpl. Erdely then stated the information about the investigations conducted by the other two computer crime investigators detailed above, including that a computer with the Subject GUID had been identified by each investigator online and sharing child pornography files. (Ex. 8)

6. Cpl. Erdely listed the January 19 IP address assigned to the Kozikowski home network as the IP address identified by Officer Paula Hoffa that was being used by the computer with

the Subject GUID to share child pornography. (Ex. 8)

7. Cpl. Erdely, however, mistakenly listed the date of Officer Hoffa's investigation as "1/19/2010" instead of the correct date of "1/19/2011" (i.e., the very day the search warrant for the Stanley residence was applied for). (59, Ex. 8)

8. Cpl. Erdely did list the correct date for the investigation conducted by Agent Jessica Eger – 1/19/2011 – and stated that Agent Eger had identified a computer with the Subject GUID sharing child pornography via the internet that very day. (Ex. 8)

9. Cpl. Erdely then went on to detail the information obtained from the investigation that he had just conducted at the Kozikowski residence and outside the Stanley residence. (Ex. 8)

10. Cpl. Erdely explained how a particular wireless device with a particular MAC address used the IP address assigned to the Kozikowski home network (i.e., the January 19 IP address). (Ex. 8)

11. Cpl. Erdely then detailed how he used Moocherhunter to follow the internet connection via the Kozikowski home network to the exterior of the Stanley residence. (Ex. 8)

12. In addition, Cpl. Erdely stated that the internet connection was communicating with the wireless device through a particular port known to be used by clients downloading files

over the Gnutella file-sharing network. (Ex. 8)

13. Cpl. Erdely also included his expert opinion that the Subject Computer was inside the Stanley residence. (Ex. 8)

14. Cpl. Erdely accurately described the Stanley residence as being part of an "apartment building" and then accurately described the part of the apartment building that contained Mr. Stanley's residence. (55-57, Exs. 5-8)

15. Cpl. Erdely did not describe the other wing of the apartment building that was not in the vicinity of the Stanley residence and not in the vicinity of where he pointed the antenna. (55-57, Exs. 5-8)

16. In the process of following the stolen internet connection to the front door of Mr. Stanley's residence, Cpl. Erdely compared the relative power meter readings until he got to the point on the nearby public sidewalk directly in front of the Stanley residence where the meter reading was 100 which is the highest possible reading. (Ex. 8)

IV. CONCLUSIONS OF LAW – SEARCH WARRANT

A. Probable Cause Was Articulated

1. The task of this Court in reviewing whether Cpl. Erdely's supporting affidavit articulated probable cause of criminal activity is to determine whether the judge who issued the search warrant had a substantial basis for concluding that contraband or evidence of criminal activity was inside the

Stanley residence. *United States v. Stearn*, 597 F.3d 540, 554 (3d Cir. 2010).

2. Probable cause exists when there is "a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Bond*, 581 F.3d 128, 139 (3d Cir. 2009) (quoting *United States v. Burton*, 288 F.3d 91, 103 (3d Cir.2002), and *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

3. Probable cause is a "commonsense, nontechnical conception[] that deal[s] with the factual and practical considerations of everyday life on which reasonable and prudent [people], not legal technicians, act." *United States v. Laville*, 480 F.3d 187, 196 (3d Cir. 2007) (citing *Ornelas v. United States*, 517 U.S. 690, 695 (1996)) (internal quotations marks omitted).

4. In reviewing a claim that probable cause of criminal activity was lacking, a reviewing court must keep in mind that there is a fundamental difference between the level of proof required to support a conclusion of guilt and the level of proof required to support a conclusion of probable cause. *Laville*, 480 F.3d at 194.

5. In fact, to find probable cause a reviewing court "need *not* conclude that it was 'more likely than not' that the evidence sought was at the place described." *Bond*, 581 F.3d at 139 (emphasis added).

6. A search warrant affidavit "should not be judged as an entry in an essay contest . . . but, rather, must be judged by the facts it contains." *United States v. Harris*, 403 U.S. 573, 579 (1971) (citation and quotation marks omitted).

7. "[S]earch warrant affidavits are normally drafted by nonlawyers in the midst and haste of a criminal investigation." *United States v. Brooks*, 594 F.3d 488, 490 (6th Cir. 2010) (citation and quotation marks omitted).

8. Cpl. Erdely drafted the supporting affidavit and the search warrant for the Stanley residence on scene and under the time crunch of obtaining judicial authorization and initiating the search prior to the evaporation of the stolen wireless connection or the flight of the subject.

9. The mistake relative to the year of the Hoffa investigation is, therefore, excusable and does not invalidate the search warrant.

10. The mistake actually contributed to Mr. Stanley's argument that there was an insufficient link between the child pornography crimes and a computer inside his residence.

11. Even with the mistaken year, the affidavit still provided a substantial basis for the judge to conclude that contraband or evidence of criminal activity was inside the Stanley residence.

12. The affidavit demonstrated that a particular computer with a

particular GUID had been observed on multiple occasions over the course of months sharing child pornography over the Gnutella file-sharing network through IP addresses assigned to the Kozikowski home network.

13. The affidavit also demonstrated that on January 19, 2011, just prior to the search warrant application, the stolen internet connection for a wireless device was followed to the Stanley residence across the street from the Kozikowski residence.

14. The affidavit explained that this wireless device was at that time receiving internet data via a port used by computers for downloading files over the Gnutella file-sharing network.

15. In addition, the affidavit included Cpl. Erdely's expert opinion that the Subject Computer was inside the Stanley residence – the issuing judge was entitled to value this opinion in light of Cpl. Erdely's expressed expertise.

16. Mr. Stanley suggests that any person could have connected to the Kozikowski home network using the Subject Computer and shared the child pornography referenced in the affidavit.

17. In light of the fact that probable cause does not require a "more likely than not" finding, the affidavit did not need to rule out the possibility that the Subject Computer could be located somewhere else as long as the affidavit provided a substantial basis for concluding that the Subject Computer was at the Stanley residence.

18. Such a substantial basis was provided by the information establishing that the Subject Computer had been used on multiple occasions over an extended period of time to share child pornography over the Kozikowski home network.

19. Such information indicated that the Subject Computer was used by a Kozikowski neighbor as opposed to someone who happened to be in the area on a particular occasion.

20. Moreover, the contemporary Gnutella port information supported a conclusion that the wireless device at the Stanley residence was the Subject Computer with the Subject Gnutella GUID.

21. Even if the affidavit failed to link the Stanley residence to the child pornography crimes, it still linked the Stanley residence to, at the very least, theft of Comcast internet services which is prohibited by the broad Pennsylvania theft of services statute reproduced below.

22. Pennsylvania prohibits such theft of services under 18 Pa.C.S.A. § 3926.

23. Section 3926(a)(1) of the Pennsylvania theft of services statute states, in pertinent part, "[a] person is guilty of theft if he intentionally obtains services for himself or for another which he knows are available only for compensation, by deception or threat, . . . by making or maintaining any unauthorized connection, whether physically, electrically or inductively, to a distribution or transmission line, by

attaching or maintaining the attachment of any unauthorized device to any cable, wire or other component of an electric, telephone or cable television system or to a television receiving set connected to a cable television system, . . . or by false token or other trick or artifice to avoid payment for the service."

24. Section 3926(a)(1.1) of the Pennsylvania theft of services statute states "[a] person is guilty of theft if he intentionally obtains or attempts to obtain telecommunication service by the use of an unlawful telecommunication device or without the consent of the telecommunication service provider."

25. The statute states that "telecommunication service . . . [i]ncludes, but is not limited to, any service provided for a charge or compensation to facilitate the origination, transmission, emission or reception of signs, signals, data, writings, images and sounds or intelligence of any nature by telephone, including cellular telephones, wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa.C.S.A. § 3926(h).

26. As previously noted, probable cause exists when there is "a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Bond*, 581 F.3d 128, 139 (3d Cir. 2009) (citation and quotation marks

omitted).

27. The search warrant was, therefore, supported not only by probable cause that child pornography evidence was inside the Stanley residence but also by probable cause that theft evidence was inside as well.

28. Mr. Stanley's computer was a seizable and searchable item regarding either type of evidence.

29. Theft of services was not listed in Cpl. Erdely's search warrant application or affidavit as the crime under investigation.

30. As the Eighth Circuit explained in *United States v. Summage*, 481 F.3d 1075, 1078-79 (8th Cir. 2007), however, "[i]t is not necessary for an affidavit to include the name of the specific crime alleged. . . . [O]nly a probability of criminal conduct need be shown." (citations and quotation marks omitted).

31. While it is certainly customary to list the crimes for which there is probable cause in an affidavit and a search warrant, it is "a fair probability that contraband or evidence of a crime will be found in a particular place" that is required to validate a search warrant, not a formal list of all crimes for which there is probable cause.

32. Therefore, even if the affidavit failed to link the Subject Computer sharing child pornography to the Stanley residence, the search warrant was still valid because the affidavit

linked the Stanley residence to evidence of the theft of the Comcast telecommunication service.

B. Search Warrant Obtained and Served in Good Faith

1. Even if the affidavit failed to articulate probable cause that evidence of a crime was inside the Stanley residence, no evidence should be excluded because the search warrant was relied upon in good faith.

2. Evidence obtained pursuant to a search warrant subsequently determined to be invalid should not be excluded when the search warrant was relied upon in objective good faith. *United States v. Tracey*, 597 F.3d 140, 150 (3d Cir. 2010).

3. In determining whether a search warrant lacking in probable cause was relied upon in good faith, facts known to the affiant that were not included in the affidavit can be considered. *United States v. Falso*, 544 F.3d 110, 127 n.22 (2d Cir. 2008); *United States v. Grant*, 490 F.3d 627, 632 (8th Cir. 2007) ("In assessing whether the officer relied in good faith on the validity of a warrant, we consider the totality of the circumstances, including any information known to the officer but not included in the affidavit. . . .").

4. "Ordinarily, the mere existence of a warrant suffices to prove that an officer conducted a search in good faith, and will obviate the need for any deep inquiry into reasonableness. Indeed, we neither expect nor require police to perform

complex legal analysis in the field, for they are untrained in the law and are often called to make hurried judgments." *United States v. Stearn*, 597 F.3d 540, 561 (3d Cir. 2010) (citations and punctuation omitted).

5. The Third Circuit has "recognized that the good faith exception does not apply in four limited circumstances: 1) where the magistrate judge issued the warrant in reliance on a deliberately or recklessly false affidavit; 2) where the magistrate judge abandoned his or her judicial role and failed to perform his or her neutral and detached function; 3) where the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or 4) where the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized." *Id.* at 151.

6. None of these four circumstances applies in Mr. Stanley's case.

7. Cpl. Erdely's knowledge that the Hoffa investigation had occurred on the same day the search warrant was obtained, instead of one year earlier, and his belief that he had correctly stated the date of the Hoffa investigation further support the conclusion that the search warrant was relied upon in good faith.

8. The correct date of the Hoffa investigation bolstered the

probable cause information in the affidavit.

9. Mr. Stanley's claim that the affidavit contained a material omission and a false statement is utterly baseless and entitles him to no relief whatsoever.

10. Cpl. Erdely accurately described the Stanley residence as being part of an "apartment building" and then accurately described the part of the apartment building that contained Mr. Stanley's residence.

11. Cpl. Erdely did not describe the other wing of the apartment building that was not in the vicinity of the Stanley residence, not in the vicinity of where he pointed the antenna, and, therefore, not relevant.

12. And, in the process of following the internet connection to the exterior of Mr. Stanley's residence, Cpl. Erdely did compare the relative power meter readings until he got to the point on the nearby public sidewalk directly in front of the Stanley residence where the meter reading was 100 which is the highest possible reading.

V. CONCLUSION

The motion to suppress must be denied. Mr. Stanley has failed to demonstrate that he had a reasonable expectation of privacy in the stolen internet connection obtained by trespass even if it led back to the front door of his residence. Therefore, the process of following it was not a search at all, let alone an unreasonable

one. Even if the process of following the stolen connection was a warrantless search, application of the exclusionary rule would be completely unjustified under the circumstances.

Furthermore, the subsequent search of Mr. Stanley's residence that resulted in the seizure of his computer was conducted pursuant to a valid search warrant. The search warrant was obtained and served in complete good faith. Mr. Stanley's claims that the search warrant affidavit contains material omissions and false statements are utterly baseless.

Respectfully submitted,

DAVID J. HICKTON
United States Attorney

s/ Craig W. Haller
CRAIG W. HALLER
Assistant U.S. Attorney
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-5870 (Fax)
craig.haller@usdoj.gov
PA ID No. 87714